International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 4, August 2020, pp. 3695~3701
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i4.pp3695-3701

Identity-based threshold group signature scheme based on multiple hard number theoretic problems

Nedal Tahat[1], Ashraf A. Tahat[2]
[1]Department of Mathematics, The Hashemite University, Jordan
[2]Department of Communications Engineering, Princess Sumaya University for Technology, Jordan

Article Info

Article history:

Received Oct 28, 2019
Revised Jan 10, 2020
Accepted Jan 29, 2020

Keywords:

Discrete logarithm
Identity-based signature
Residuosity
Threshold signature

ABSTRACT

We introduce in this paper a new identity-based threshold signature (IBTHS) technique, which is based on a pair of intractable problems, residuosity and discrete logarithm. This technique relies on two difficult problems and offers an improved level of security relative to an on two difficult hard problems. The majority of the denoted IBTHS techniques are established on an individual difficult problem. Despite the fact that these methods are secure, however, a prospective solution of this sole problem by an adversary will enable him/her to recover the entire private data together with secret keys and configuration values of the associated scheme. Our technique is immune to the four most familiar attack types in relation to the signature schemes. Enhanced performance of our proposed technique is verified in terms of minimum cost of computations required by both of the signing algorithm and the verifying algorithm in addition to immunity to attacks.

Corresponding Author:

Nedal Tahat,
Department of Mathematics,
The Hashemite University,
Zarqa 13133, Jordan.
Email: nedal@hu.edu.jo

1. INTRODUCTION

In 1971, the idea of digital signature was first presented by Diffie and Helman [1] that enabled a signer in possession of a secrete key to sign a message, while anybody using a public key could perform verification of the signature. The notion of threshold signatures was presented by Desmedt [2] in 1987. A secret key, and correspondingly, the signing power, is shared to a collection of n players in a (t,n) threshold signature scheme, where this is accomplished in a manner that any subset of t players is able to collectively deliver a signature on the account of the group, whereas a subset composed of up to $t-1$ players is incapable. The threshold signature is fundamental yet of a great significance cryptographic scheme that is due to its bifold function: by boosting the opportunity of the signing agency while simultaneously improving the safeguarding process against fraudulence through completing the learn process of the secret signature key for the antagonist. Subsequent to Desmedt's creation, in the commonly-named threshold cryptography domain, several threshold signature approaches incorporated on diverse premise were formulated, such as [3-8]. In order to streamline key management processes in certificate based public key setting, Shamir [9] in 1984, called for identity-based (ID-based) encryption and signature methods. Thenceforth, in the scope of this commonly-named ID-based cryptography, scores of identity-based cryptography techniques were put forward, such as the works of [10, 11]. The remarkably prominent tool has proposed bilinear pairing [10] in constructing identity-based cryptography primitives, where ID-based could be substituted for certificate-based in public key setting. This is of a special interest particularly when there is a requirement for efficient key management while moderate security is needed. The entire developed literature put forward on ID-based threshold group signature contains approaches that rely on an individual hard problem such as factoring,

discrete logarithm or elliptic curve discrete logarithm problem [1-20]. Hereafter, if a solution of any of these problems is achieved, then the security of the associated ID-based threshold group signature would be compromised. Therefore, we present in this work a secure ID-based threshold group signature incorporated on discrete logarithms and residuosity problem. Our techniques enhancement arises from the difficulty in finding simultaneous solution of both problems. We demonstrate that our approach persists to be secure, despite attaining solution of one of the problems. The remainder of the paper is structured as follows: the IBTHS is introduced in Section 2. Section 3 presents security analysis of our technique. Performance study and resultant efficiency are carried out in Section 4. Finally, we conclude in Section 5.

2. THE PROPOSED IBTHS

Here, we will introduce our identity based threshold signature technique that relies on a pair of hard number theoretical problems; namely, residuosity and discrete logarithm. As was stated, the security if this technique builds on the premise that it is burdensome to simultaneously achieve solutions of this pair of problems. The framework of our technique presumes, t out of n signers are able to jointly sign the message on the account of the group, whereas an individual verifier is able to corroborate the group signature [21].

2.1. System setup

The trusted dealer (TD) of the system, following the framework of [21], selects a large prime p- a 1024-bits, $N = p_1 q_1$ is a factor of $p - 1$, where p_1 and q_1 are two safe primes, an element g generator of order N, adhering to $g^N \equiv 1 \pmod p$, and where $h(m)$ is the one-way hash function for the message m.

2.2. Generating keys

Within this stage, TD carries-out the consecutive operations [21] to produce the secret and public keys of the technique:

- Selects in a random fashion: $\lambda \in z_N^*$ such that $\gcd(\lambda^2, N) = 1$
- Calculate $\alpha \equiv g^{\lambda^2} (mod\ p)$
- After that, construct a (t, n) threshold function $f(x) = a_\circ + a_1 x + \cdots + a_{t-1} x^{t-1} (\text{mod } N)$, where a_i are random integers between 1 and $N - 1$, and $i = 0,1,2, \dots, t - 1$
- Set the group secret key (0) , then compute the associated group public key $Y = g^{f(0)} (\text{mod } p)$
- Each of the group members picks an integer $x_i \in GF(p)$ in a random manner as his private key and calculates his public key: $y_i = g^{x_i} (mod\ p)$.
- Each participant registers an identity ID_i and then sends ID_i to TD.
- After TD obtains the complete identities, s/he calculates: $f(ID_i)$ and $Y_i = g^{f(ID_i)} (\text{mod } p)$ and forwards $f(ID_i)$ to the group's members individually. Public Y_i and retain a copy of $(ID_i), Y_i$.

In the event that an extra member u_i wishes to participate within the group following negotiation with the TD, s/he posts her/his identity ID_i to the TD. After which, TD calculates and transmits $f(ID_i)$ to her/him. Then, TD calculates and publics: $Y_i = g^{f(ID_i)} (\text{mod } p)$. The public and secret keys for an individual represented as (Y_i, y_i) $(f(ID_i), x_i)$, respectively. While for group, the public and secret keys are (α, Y) and $(\lambda, f(0))$, respectively.

2.3. (t,n) Threshold signature generation phase

Consider a scenario where the t members that cooperate in producing the signature [21] are $u_1, u_2, \dots, u_t$. Ahead to their collaborative signature of the message, a selected member is appointed as a clerk to perform partial signature verification. The sequential steps of message signing are illustrate as follows:

a. Each signer selects $k_i \in z_N^*$ and computes

$$r_i \equiv g^{x_i k_i} (mod\ p) \quad (1)$$

b. The $\{r_i\}$ broadcasted to members by means of a channel that is secure. When entire r_i are acquired, they are utilized collectively in the computation of the value R as

$$R = \prod_{i=1}^{t} r_i \ (mod\ p) \quad (2)$$

c. Calculate

$$v_i \equiv \left(h(m) f(ID_i) \prod_{j=1, j \neq i}^{t} \frac{-ID_i}{ID_i - ID_j} - x_i k_i \, R \right) \text{mod } N \quad (3)$$

Then send R along with (r_i, v_i) as the partial signature for the hash-function message $h(m)$ to the clerk. Later, the clerk performs validation of the partial signature through demonstrating that the subsequent equality is fulfilled:

$$g^{v_i}\, r_i^{R} = Y_i^{h(m)\prod_{j=1,j\neq i}^{t}\left(\frac{-ID_i}{ID_i-ID_j}\right)} \pmod p \tag{4}$$

d. Following demonstrating the validity of all partial signatures by the clerk, s/he obtains solution for:

$$V^2 = \lambda^{-2}\sum_{i=1}^{t} v_i \ (mod\ N) \text{ for } V \tag{5}$$

and the signature of message m is $\{R, V\}$.

2.4. (t,n) Threshold signature verification phase

The signature can be verified by a stranger pending that s/he can get a hold of to the public key [21]. Following to their reception of the group signature $\{R, V\}$ s/he examines the equation:

$$\alpha^{V^2} R^R = Y^{h(m)} \pmod p \tag{6}$$

If this condition is fulfilled, accordingly the group signature is valid.

Theorem 1. Succeeding the utilized protocol, thus the verification within the signature verification part is accomplished.

$$\begin{aligned}
\alpha^{V^2} R^R &\equiv \left(g^{\lambda^2}\right)^{\lambda^{-2}\sum_{i=1}^{t} v_i}\, R^R \pmod p \\
&\equiv g^{\sum_{i=1}^{t} v_i}\, R^R \\
&\equiv g^{\sum_{i=1}^{t}\left(h(m)f(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_i}{ID_i-ID_j} - x_i k_i R\right)}\, R^R \\
&\quad g^{\sum_{i=1}^{t}\left(h(m)f(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_i}{ID_i-ID_j}\right)} g^{-\sum_{i=1}^{t}(x_i k_i R)}\, R^R \\
&\equiv \left(g^{\sum_{i=1}^{t} f(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_i}{ID_i-ID_j}}\right)^{h(m)} \left(g^{\sum_{i=1}^{t}(x_i k_i)}\right)^{-R}\, R^R \\
&\equiv \left(g^{f(0)}\right)^{h(m)} R^{-R} R^R \pmod p \\
&\equiv Y^{h(m)} \pmod p
\end{aligned} \tag{7}$$

3. SECURITY ANALYSIS

We demonstrate here that the presented scheme for identity–based threshold signature is unforgeable found on the complexity of finding solutions simultaneous to the pair of hard number theoretical problems; residuosity and discrete logarithm. Forth while, we shall substantiate that our technique is heuristically secure against example cryptographic attacks [21].

Attack 1: Suppose that the adversary (Adv) attempts to acquire the secret keys $\lambda, f(0)$ taken from the equations $\alpha \equiv g^{\lambda^2}(mod\ p)$ and $= g^{f(0)} (\text{mod } p)$. It is evidently infeasible in view of the hindrance of figuring out residuosity and discrete logarithm problems. Also Adv cannot derive the secret key $f(ID_i)$ from the equation $Y_i = g^{f(ID_i)} (\text{mod } p)$ by virtue of the complication of solving DLP.

Attack 2: Assume that the discrete logarithm problem can be figured-out.

- By means of the equation $\alpha^{V^2}(mod\ p)$, Adv can find $V^2(mod\ N)$. Nonetheless, s/he is still incapable of recovering V because of the adversity of solving residuosity problem.
- Adv may likewise attempt to figure-out the entire secret keys of the signer utilizing the relationship $Y_i = g^{f(ID_i)} (\text{mod } p)$. Considering that discrete logarithm can be figured-out, at that point s/he can discover all secret keys (ID_i) , and thereafter construct the entire partial signature of the group. Although,

s/he is unable to identify the group signature V through the relationship $V^2 = \lambda^{-2} \sum_{i=1}^{t} v_i \ (mod\ N)$ due to the fact that s/he is not aware of the prime factorization of N.

Attack 3: Assume that the residuosity problem is solvable. In this situation, s/he has knowledge of the prime factorization, p_1 and q_1. Consequently, s/he will attempt to figure-out the formula $\tau \equiv \alpha^{V^2}(mod\ p)$. Nevertheless, s/he remains incapable of figuring-out V relying on this condition due to the fact that s/he is not aware of $V^2(mod\ N)$ for the reason that a discrete logarithm problem can not be unraveled.

Attack 4: Adv can in addition attempt to gather t pairs of message –signature (r_{ij}, v_{ij}) and m_j where $j = 1,2, \dots, t$ also tries to seek-out the individual secret key (ID_i) . Meanwhile, Adv possesses t equations in this fashion:

$$v_{i1} \equiv \left(h(m_1) f(ID_i) \prod_{j=1, j\neq i}^{t} \frac{-ID_i}{ID_i - ID_j} - x_i k_{i1}\, R_1 \right)$$

$$v_{i2} \equiv \left(h(m_2) f(ID_i) \prod_{j=1, j\neq i}^{t} \frac{-ID_i}{ID_i - ID_j} - x_i k_{i2}\, R_2 \right)$$

$$v_{it} \equiv \left(h(m_t) f(ID_i) \prod_{j=1, j\neq i}^{t} \frac{-ID_i}{ID_i - ID_j} - x_i k_{it}\, R_t \right) \quad (8)$$

The number of unknowns is $(t + 2)$ in the previous t formulas of (8), i.e., (ID_i) , x_i and k_{ij}. Hence, $f(ID_i)$ and x_i remain complex to identify considering that Adv can reproduce a limited number of solutions to this set of linear equations although s/he is not capable of identifying which is the right one.

Attack 5: Adv could seek to pose as signer u_i by choosing in a random fashion integers $x_i k_i$ and announcing g $r_i \equiv g^{x_i k_i}(mod\ p)$. Because the entire t signers decided on the group signature, in the absence of knowledge of the respective secret key $f(ID_i)$, Adv is incapable of generating a correct partial signature (r_i, v_i) to fulfill the verification formula.

Attack 6: Adv may contend to evolve a group signature (V, R) of his own using the verifying equation $\alpha^{V^2} R^R = Y^{h(m)}(mod\ p)$ for a specific message m through fixing one integer, while seeking to identify the other. In this scenario, Adv picks R and seeks the value of V. Adv begins by calculating $\rho \equiv Y^{h(m)} R^{-R}(mod\ p)$ and finding $\rho \equiv \alpha^{V^2}(mod\ p)$ for V . Unsuccessfully, s/he is unable to figure-out V utilizing this equation because of the adversity of figuring-out, simultaneously, the residuosity and discrete logarithm problems. In addition, Adv could attempt to set V and figure-out R. In this situation, s/he computes $\mu \equiv Y^{h(m)} \alpha^{-V^2}(mod\ p)$ and seeks out a solution to $\mu \equiv R^R(mod\ p)$. This scenario is the worst due to the fact that although both problems of residuosity and discrete logarithm can be solved, the R value remains difficult to determine aside from a trial and error procedure, thus characterized by consumption of time and effort [15].

4. PERFORMANCE EVALUTION

To investigate the performance of identity-based threshold signature, computation and communication overheads will be used to estimate it. Here, we will examine primarily the performance of our suggested technique. To facilitate this treatment, we employ the following notations in our analysis of the computation and communication complexity [22-25]. The number of secret and public keys are denoted by SK and PK, respectively. Modular exponentiation time is represented by; T_{exp} , while T_{mul} stands for the time for modular multiplication; and the time for a modular inverse computation is represented by T_{inv} ; T_{sq} denotes complexity of time for executing computation of the modular square; T_{sqr} presents the complexity for executing calculation of the modular square root. T_h determines the one map-to-point hash function time, while $|x|$ specifies the length of bits of x. We must note that other computational operations times are ignored, since they are much smaller than T_{exp} , T_{mul}, T_{sq} and T_h . We summarize the computation and communication cost of our proposed scheme in Table 1. As shown in Table 1, the computation complexity [22] for signature and verification are $4tT_{exp} + (4t^2 + t + 1)$+$(t^2 - t + 1)T_{inv} + T_{sq} + T_{sqr} + T_h$and $3T_{exp} + T_{mul} + T_{sq} + T_h$ in our scheme, respectively. Also the total communication cost are $(2t + 1)|N| + (3t + 1)|p|$.

Table 1. The performance of our scheme

Criteria		Evaluation
No. of keys	SK	$2t+1$
	PK	2t+1
Computational complexity	Sign	$4tT_{exp}+(4t^2+t+1)T_{mul}+(t^2-t+1)T_{inv}+T_{sq}+T_{sqr}+T_h$
	Verify	$3T_{exp}+T_{mul}+T_{sq}+T_h$
Size of parameters/communication cost		$(2t+1)\|N\|+(3t+1)\|p\|$

5. ILLUSTRATION

To illustrate the proposed scheme, we consider that there are three users. The trusted dealer (TD) of the system choose $p=14447, p_1=31, p_2=233$, then $N=p_1p_2=7223$, $g=8$ and $h(m)=801$. The following step illustrate our scheme.

5.1. Keys generation

In this step, the subsequent actions are carried-out by TD to generate the scheme's secret and public keys:

a. Selects in a random fashion $\lambda=223\in z_N^*$ and observing that $\gcd(\lambda^2,N)=1$. Calculate $\alpha\equiv 8^{6391}\text{mod}14447\equiv 8853 \bmod 14447$. Select a polynomial $f(x)=311+733x+123x^2(\bmod 7223)$. Set the group secret key $f(0)=311$ and calculates the corresponding group public key $Y=8^{311}\bmod 14447\equiv 10022 \bmod 14447$.
b. Each of the three members of the group, in a random fashion, picks an integer as: $x_1=163, x_2=237, x_3=757$, to represent his private key, and then determines his public key $y_1=8^{163}\bmod 14447\equiv 5619, y_2\equiv 8^{237}\bmod 14447\equiv 2811, y_3\equiv 8^{757}\bmod 14447\equiv 1670$.
c. Each participant registers an identity $ID_1=321, ID_2=531, ID_3=239$ and then sends ID_i to TD. TD computes and publics

$$Y_1\equiv g^{f(ID_1)}\bmod p\equiv 8^{2146}\text{mod } 14447\equiv 8300$$

$$Y_2\equiv g^{f(ID_2)}\bmod p\equiv 8^{3072}\text{mod } 14447\equiv 8450$$

$$Y_3\equiv g^{f(ID_3)}\bmod p\equiv 8^{50}\text{mod } 14447\equiv 1543$$

5.2. (t,n) Threshold signature generation phase

Assume that the t members participating in the signature generation are $u_1,u_2,\dots,u_t$. Preceding to jointly signing the message, one of these members is appointed as a clerk to perform verification the partial signature. We describe the elements of message signing in sequence as follows:
Each signer selects $k_1=117, k_2=147, k_3=371$ and computes

$$r_1\equiv 8^{163(117)}\bmod 14447\equiv 10094$$

$$r_2\equiv 8^{237(147)}\bmod 14447\equiv 2746$$

$$r_3\equiv 8^{757(371)}\bmod 14447\equiv 1247$$

The $\{r_i\}$ are broadcasted through a secure channel to the members. Subsequent to reception of the entire r_i, each of them computes the value R as $R=\prod_{i=1}^{3}r_i\,(mod\ p)=(10094\times 2746\times 1247)\bmod p\equiv 9787$ Calculates $v_1=5195,\ v_2=3174, v_3=1583$.
Then send R along with (r_i,v_i), representing the hash-function message $h(m)$ partial signature, to the clerk. Subsequent to validation of entire partial signatures by the clerk, s/he determines solution of $V^2=\lambda^{-2}\sum_{i=1}^{t}v_i\ (mod\ N)$ for V, $V^2=1172(2894)\text{mod } 7223\equiv 4181$.

5.3. (t,n) Threshold signature verification phase

Any newcomer is able to perform verification of the signature granted that s/he can access the public key. Succeeding to his reception of the group signature, $\{R,V\}$ he reviews:

$$\alpha^{V^2}R^R=Y^{h(m)}\ (\bmod p)$$

$$\alpha^{V^2}R^R\equiv 8853^{4181}9787^{9787}(\bmod 14447)\equiv 3768$$

$$Y^{h(m)}\equiv 10022^{801}(\bmod 14447)\equiv 3768$$

6. CONCLUSION

A new technique for ID-based threshold group signature was proposed, which is founded on the problems of residuosity and discrete logarithm. The technique relies on two difficult hard problems and offers an improved level of security relative to an individual difficult problem. Also, we have investigated some potential attacks and demonstrated the security of the scheme against such attacks. In addition, the scheme is resistant to both of repeat and conspiracy attacks. Moreover, each of group signature and group key sizes do not rely on the number of members.

REFERENCES

[1] W. Diffie, M. E. Hellman, "New direction in Cryptography," *IEEE Transaction on Information Theory*, vol. 22, pp. 644-654, 1971.

[2] Desmedt, "Society and group oriented cryptography: A new concept," *In Proc. A Conference on the Theory and Applications of Cryptographic Techniques*, Santa Barbara, USA, pp. 120-127, 1987.

[3] A. Boldyreva, "Efficient threshold signatures, multi- signatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme," *In Proceedings of PKC 2003,* Miami, USA, pp. 31-4, 2003.

[4] Y. Desmedt, "Threshold cryptography," *European Transactions on Telecommunication*, vol. 5, no. 4, pp. 449–457, 1994.

[5] P. A. Fouque and J. Stern, "Fully distributed threshold RSA under standard assumptions," *In Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security*, Gold Coast, Australia, pp. 310-330, 2001.

[6] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, "Robust threshold DSS signatures," *Information and Computation*, vol. 164, no. 1, pp. 54–84, 2001

[7] V. Shoup, " Practical threshold signatures, "*In Proceedings of International Conference on the Theory and Application of Cryptographic Techniques*, Bruges, Belgium, pp. 207-220, 2000.

[8] J. Yu, F. Kong X, Cheng, "Forward-secure multisignature, threshold signature and blind signature schemes," *Journal of Networks*, vol. 5, no. 6, pp. 634-641, 2010.

[9] V. Shamir, "Identity-based cryptosystems and signature schemes," *In Proceedings of Crypto* 1984, Santa Barbara, USA, pp. 47-53, 1984.

[10] M. Bellare, Namprempre C. and G. Neven, "Security proofs for identity based identification and signature schemes," *In Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques*, Interlaken, Switzerland, pp. 268-286, 2004.

[11] D. Boneh, and M. Franklin, "Identity-Based encryption from the Weil pairing," *In it Crypto 2001, Santa* Barbara, USA, pp. 213-229, 2001.

[12] F. Li, J. Yu, "A New Threshold Group Signature Scheme Based on Discrete Logarithm Problem," *Eighth ACIS International Conference Network and Parallel/Distributed Computing, SNPD 2007*, vol. 3, pp. 1176-1182, 2007.

[13] Y. Yu, B. Yang, Y. Sun, "Identity-based threshold signature and mediated proxy signature schemes," *Journal of China Universities of Posts and Telecommunications*, vol. 14, no. 2, pp. 69–74, 2007.

[14] Q. Huawang, Z. Xiaohua, D. Yuewei, "Provably secure Identity-based threshold signature on access structure," *International Conference on Information and Communications Technologies*, 2014.

[15] L. Deng and J. Zeng, "Two new identity-based threshold ring signature schemes," *Theoretical Computer Science*, vol. 535, pp. 38-45, 2014.

[16] N. Tahat, "Convertible multi-authenticated encryption scheme with verification based on elliptic curve discrete logarithm problem, "*Int. J. Computer Applications in Technology*, vol. 54, no. 3, pp. 229-235, 2016.

[17] S. Chang, D. S. Wong, Y. Mu, Z. Zhang, "Certificateless Threshold Ring Signature,*" Information Sciences*, vol. 179, pp. 3685–3696, 2009.

[18] H. Xiong, J. Hu, Z. Chen, F. Li, "On the security of an identity based multi-proxy signature scheme," *Computers and Electrical Engineering*, vol. 37, pp. 129-135, 2011.

[19] L. Fagen, H. Yupu, C. Jie, "Improvement of Identity.Based Threshold Proxy Signature Scheme with Known Signers," *Wuhan University Journal of Natural Sciences*, vol. 11, no. 6, pp. 1653-1656, 2006.

[20] Y. Yong, L. Fagen, X. Chunxiang, S. Ying, "An Efficient Identity-Based Anonymous Signcryption Scheme,*" Wuhan University Journal of Natural Sciences*, vol. 13, no. 6, pp. 670-674, 2008.

[21] M. Mohamad and E. Ismail, "Threshold Signature with Hybrid Problems," *International Journal of Cryptology Research*, vol. 4, no. 1, pp. 32 - 41, 2013.

[22] E.S, Ismail, N.M.F. Tahat, and R.R Ahmad, "A New Digital Signature Scheme Based on Factoring and Discrete Logarithms," *Journal of Mathematics and Statistics*, vol. 4, no. 4, pp. 222-225, 2008.

[23] N. Tahat, R. Shaqboua, E. Abdallah, M. Bsoul and Wasfi Shatanawi, "A new digital signature scheme with message recovery using hybrid problems," *International Journal of Electrical and Computer Engineering*," vol. 9, no. 5, pp. 3576-3583, 2019.

[24] N. Tahat and M. S. Hijazi, "A New Digital Signature Scheme Based on Chaotic Maps and Quadratic Residue Problems," *Applied Mathematics & Information Sciences*, vol. 13, no. 1, pp. 115-120, 2019.

[25] N. Tahat, A. A. Tahat, M. Abu-Dalu, R. B. Albadarneh, A. E. Abdallah and O. M. Al-Hazaimeh," A new RSA public key encryption scheme with chaotic maps," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 1430-1437, 2020.

BIOGRAPHIES OF AUTHORS

Nedal Tahat received his BSc in Mathematics from Yarmouk University, Jordan in 1994, and MSc in Pure Mathematics at Al al-Bayt University, Jordan, in 1998. He received a PhD in Applied Number Theory (Cryptography) from National University of Malaysia (UKM) in 2010. He is an Associate Professor in the Department Mathematics, Hashemite University. His main research interests are cryptology and number theory. He has published more than 35 papers, authored/coauthored, and more than 15 refereed journal and conference papers

Ashraf A. Tahat is an Associate Professor in the Department of Communications Engineering at Princess Sumaya University for Technology (PSUT) and the Vice-Chairman of IEEE Jordan Section. Dr. Tahat earned his B.Sc. and M.Sc. degrees in Electrical Engineering from the Illinois Institute of Technology (IllinoisTech), Chicago, USA, where he also received a Ph.D. in 2002, with a focus on communications and signal processing. Dr. Tahat joined PSUT in 2005 and served as the Head of the department of Communications Eng. from 2010 to 2012. He was also a Visiting Professor with McGill University, Montreal, Canada, in the Department of ECE, conducting research on modern communications systems (2012-2013). From 2002 to 2003, he was an Adjunct Professor at IllinoisTech, Chicago, USA.